Statement of

Vincent Weafer
Senior Director of Security Response
Symantec Corporation

Before the
Subcommittee on Telecommunications and the Internet
Committee on Energy and Commerce
United States House of Representatives

Hearing on
Cybersecurity: Protecting America's Critical Infrastructure, Economy and Consumers

September 13, 2006

Overview

Chairman Upton, Ranking Member Markey, distinguished members of the Subcommittee: Thank you for inviting me here today to testify about protecting our nation's critical infrastructure and the opportunity to provide you with an overview of the current cyber threat landscape. My name is Vincent Weafer and I am the Senior Director of Security Response for Symantec Corporation.

I'd like to begin by commending the Subcommittee for bringing attention to this critical issue. It's vitally important that we pay attention to the threats to our nation's security including the clear and present danger of potential cyber attacks against our nation's information infrastructure.

Our society's increasing dependence on computers means that the disruption of our networks whether due to nation-states, terrorists, criminals, or simply pranksters could seriously impair public safety, national security, economic prosperity and, more generally, our way of life. An attack against the information technology backbone of one of our nation's so-called critical infrastructures such as communications services, energy, financial services, manufacturing, water, transportation, health care, and emergency services could disrupt Americans physical and economic well-being and have a worldwide impact. An attack against the U.S. that combines both cyber and physical elements could be particularly devastating, such as a physical attack against a building combined with disruption of the telecommunications infrastructure needed to provide emergency services to the physically affected area.

Accordingly, I would like to devote my testimony today to two issues. I would first like to provide this Subcommittee with Symantec's updated assessment of our nation's cyber security landscape and discuss the vulnerabilities of the U.S. information infrastructure to cyber attacks.

Second, I'd like to discuss the considerable negative impact that cybercrime is having on undermining consumer trust which in turn is eroding the publics' confidence in performing commerce over the Internet. Finally, I will discuss the economic consequences that cyber attacks are having on the U.S. economy.

Background on Symantec

Before I turn to the main substance of my testimony, I would like to provide you background on Symantec Corporation. Symantec is the global leader in information security. We provide solutions to help individuals and enterprises assure the security, availability and integrity of their information. Symantec's Norton brand of products is the worldwide leader in consumer security and problem solving solutions. Headquartered in Cupertino, California, Symantec employs over 15,000 professionals and has operations in more than 40 countries.

I am responsible for the Symantec Security Response global research teams. My mission is to advance the research into the new Internet security threats and to provide the most trusted and rapid response to today's complex threats, security risks and cyber attacks. Symantec Security Response protects a variety of businesses, consumers and government agencies from the latest security threats. Symantec Security Response consists of dedicated intrusion experts, security engineers, virus hunters, and global technical support teams that provide our customers with comprehensive, global, 24x7 Internet security expertise to guard against today's complex Internet threats.

Symantec gathers our research from our "Global Intelligence Network" which consists of more than 40,000 sensors monitoring activity on computers in more than 180 countries. We gather data from over 120 million computer systems that use Symantec's anti-virus products and probe over 2 million decoy email accounts. Symantec also operates 4 cyber Security Operations Centers spread across the globe – including Alexandria, Virginia; London, England; Munich, Germany; and Sydney, Australia – each dedicated to relentlessly searching the Internet for potential cyber threats 24 hours a day, 365 days a year to provide managed, pre-emptive protection for our customers. If there is a class of threat on the Internet Symantec knows about it.

State of the Nation's Cyber Security Landscape

As the company representative of the security technology industry on this morning's panel, I want to stress an important message about our nation's cyber security landscape: First, the threats to our critical infrastructure are absolutely real and, without a doubt, growing. The question is not if or even when we'll be attacked but how severe will the attack be.

Today, I stand before you to say that the threat has changed.

The main risks to information these days are not the large-scale, fast-moving virus or worm pandemic type attacks that we saw with frequency just a couple years ago. Consider this: from 2002 to 2004, there were almost 100 medium-to-high risk attacks. Last year, there were only six and so far in 2006, there have been none.

What happened?

We've made significant headway in containing and repelling these sorts of threats. And an equally big part is that the very nature of the risks we face has changed. In the past, cyber attacks were largely

designed to destroy data or gain notoriety, but today's attacks are increasingly designed to silently steal data for profit or advantage, without leaving behind the system damage that would be noticeable to a user.

Fraud, intelligence gathering and gaining access to vulnerable systems are the motivation behind many of today's attacks. The attackers are not interested in notoriety. They're interested in flying below the radar, using lower profile, more targeted attacks, attacks that propagate at a slower rate in order to avoid detection and thereby increase the likelihood of successful compromise. Instead of exploiting vulnerabilities in servers, as traditional attacks often did, these threats tend to exploit vulnerabilities in client-side applications that require a degree of user interaction, such as word processing and spreadsheet programs. A number of these have been zero-day vulnerabilities. These types of threats also attempt to escape detection in order to remain on host systems for longer periods so that they can steal information or provide remote access. They're increasingly interested and capable of perpetrating silent, highly-targeted attacks to steal sensitive personal, financial, and operational information using data mining techniques to identify the victims and improve the effectiveness of the attack.

Cybercrime is the dominating security threat we're seeing today and there's been a marked increase in the use of "crimeware". Crimeware is software built with the purpose of committing online scams and stealing information; it includes (but is not limited to) bots, keystroke loggers, spyware, backdoors, and Trojan horses or software used to conduct cybercrime.

Symantec just compiled the latest cyber threat data for our tenth Internet Security Threat Report, or ISTR, which is widely acknowledged to be the most comprehensive analysis of security activity for today's information economy. The Report includes an analysis of network based attacks on the Internet with a review of known threats, vulnerabilities, and highlights of malicious code and additional security risks. Symantec has provided this Report semi annually since 2002.

The ISTR also offers security best practices for consumers and businesses to help them protect against current and emerging cyber crime threats. Symantec's ISTR found that the last 6 months have seen growth in attack trends, bot infections denial of service attacks, malicious code such as Trojans and phishing attacks.

Symantec's ISTR found that attackers are moving away from large, multiple purpose attacks against traditional security devices such as firewalls and routers. Instead, they are focusing their efforts on regional targets, desktops and Web applications that may allow an attacker to steal corporate, personal, financial, or confidential information; this information could then be used for additional criminal activity. Attackers are focusing not just on the end users systems via exploitable browser vulnerabilities, but also

on weaknesses in the web servers and web applications. They can use that weakness to drop malicious code such as a keyboard logger onto a users system, when the unwitting and unprotected user browses or 'drives-by' the compromised Web site. This attack impacts both the end user privacy, as well as the brand name of the company whose Web presence has been compromised.

Programs that provide attackers with unauthorized control of a computer, known as bots, also contribute to the rise in cybercrime threats. Symantec's March 2006 Internet Security Threat Report identified an average of 9,163 infected computers each day—bot networks are being increasingly used for criminal activities such as DoS-based extortion attempts. We believe we will see a continuing growth trend in the area of botnet infected computers. During that period, the United States had a very high percentage of the bot command-and-control servers worldwide. Symantec expects this trend to continue.

Botnets are the engine that drives most of the criminal activity, as they get used by to distribute Spam, Phishing messages, malicious code as well as storage for illegal material. Many of these botnets are created on systems owned by home users, small businesses and even some large corporations.

Symantec estimates that the measurement above is only capturing a portion of global activity and that the actual infection numbers are likely to be much higher. In our March 2006 Internet Security Threat Report Symantec identified an average of 1,402 DoS attacks per day—a 51 percent increase over the previous reporting period. Our Reports consistently show that the United States was the target of the most DoS attacks, accounting for over half of the worldwide total.

We believe that this growth trend will continue as attackers leverage an increasing number of Web-based application and browser vulnerabilities.

In Symantec's March 2006 ISTR, we saw, attacks directed at Web application technologies increase—69 percent of the vulnerabilities reported to Symantec affected Web application technologies, a 15 percent increase over the previous reporting period. The new report does see a significant amount of attacks targeted. We found that Web application technologies, which rely on a browser for their user interface, present an easier target for attackers due to their availability over commonly allowed protocols such as HTTP.

Symantec has also consistently seen an increase in modular malicious code, which initially possesses limited functionality but is designed to update itself with new, more damaging capabilities. Modular malicious threats often expose confidential information that can then be used in identity theft, credit card fraud, or other criminal financial activities. According to our March 2006 ISTR, malicious code that could reveal confidential information rose from 74 percent of the top 50 malicious code samples last

reporting period to 80 percent this period—an increase of 6 percentage points. Symantec expects this growth to continue to increase in future reporting periods.

These criminals are targeting all sorts of organizations. By leveraging the vast number of new vulnerabilities, the potential introduction of entirely new and more destructive forms of malicious code and cyber attacks tools represents a substantial future risk. Our law enforcement, military and national security agencies face an even more sophisticated threat with all of these new vulnerabilities, zero day attacks and highly targeted attacks.

Right now, more than 20 nations possess dedicated computer attack programs – and that number doesn't include terrorist organizations.[1] Cyber warfare is a part of their war plans.

Indeed, in the first half of 2004, DoD experienced more than 150 hostile intrusion attempts per day. In the first half of 2005, that number was up to more than 500 a day.[2]

More specifically, cybercriminals could attack our computer systems in a variety of ways, causing serious consequences including: (1) compromising the integrity of data, such as deleting records of financial institutions; (2) breaching the confidentiality of data, such as obtaining information from power and energy plants which can then be used to plan a physical attack; and (3) acting as weapons of mass disruption to take-down key Internet nodes whose failure would then lead to a cascading effect, meaning wide-ranging disruption of other parts of our critical infrastructures, or more likely impacting our ability to respond to a physical event.

The Economic Impact of Cyber Attacks and the Undermining of U.S. Consumer Confidence in Using the Internet for Commerce

Unless a trusted relationship exists between businesses and consumers the risks associated with online transactions will become unacceptable. So, the expectations are high. And, the stakes are enormous.

Across industries, companies have built into their business models the efficiencies of these new digital technologies – such as real-time tracking of packages and online commerce. The continued expansion of the digital lifestyle is already built into almost every company's assumptions for growth – and underpins the assumptions for the global economy.

---

[1] "Information Battleground," *Air Force Magazine*, http://www.afa.org/magazine/Dec2005/1205info.asp.
[2] "Information Battleground," *Air Force Magazine*, http://www.afa.org/magazine/Dec2005/1205info.asp.

Think about what would happen if banks were forced to stop all online banking and go back to the days of long lines at teller windows. The costs would be enormous. Today, it costs a bank $10 when a consumer originates a loan online. That cost jumps to more thank $200 when the loan is originated through a branch office.

We can't go back to the old way of doing business – and, that's why creating confidence in the digital world is everybody's job. For the individual company, failure to protect their customers' information will result in customers simply taking their business someplace else, to someone they can trust. And they won't necessarily turn to the company around the corner. In the global economy, security can be a competitive advantage – or disadvantage. If consumers can't trust businesses from our country, they'll look all over the world for the one's they believe they can trust. In such a world, security guarantees are very likely to trump the comfort of the local brand.

If we fail to create a trusted digital environment, we won't just slow the growth of e-business, but of all business. We won't just hurt the digital economy, but the economy as a whole. And this is the real hidden threat today – not some massive cyber attack, but the loss of consumer confidence in the digital world.

The IT industry has made huge strides these past few years, and from the evidence at hand we've made significant headway in controlling large-scale, fast moving viruses and worms. The broad adoption of best security practices and defense in-depth strategies, deployment of firewall, antivirus, and intrusion detection software and the progress operating system vendors have made in improving the security of their operating system platforms have made this possible. Mitigating the large scale virus and worm challenge is a major accomplishment but those are yesterday's problems.

Today we face a bigger challenge. As vendors and enterprises have adapted to the changing threat environment this has resulted in more targeted malicious code and targeted attacks aimed at client-side applications, such as Web browsers, email clients, and other applications. These applications are used to communicate over networks and interact with Web-based services and applications and Web sites. Today's threats are silent and highly targeted. They take advantage of the naiveté and inexperience of many online users. For example, attackers set up fake Web sites with relative ease and dupe people into offering up financial information or making a donation to a bogus charity. And of course, there are the large scale data breaches – some innocent, some inside jobs, and some the work of skilled criminals – that have made identity theft a growing threat to the digital lifestyle.

For six consecutive years, identity theft has topped the annual list of consumer complaints collected by the Federal Trade Commission. Over the past year more than 52 million records of Americans' private personal information – an average of 142,000 per day – have been hacked into, lost, stolen or otherwise compromised from digital databases.

The cost of these breaches, in terms of time and money, is astounding. According to the Federal Trade Commission identity theft costs businesses $48 billion annually, and last year cost consumers $680 million in losses. On top of that, identity theft victims collectively spent almost 300 million hours trying to repair damage.

It is difficult to quantify the economic impact of cyber crime but according to the FBI's 2005 Cyber Crime Survey cyber crime costs about $67 billion to U.S. firms over the last year. A Report by the Congressional Research Service found that investigations into the stock price impact of cyber-attacks show the identified target firms suffer losses of 1%-5% in the days after an attack. For the average New York Stock Exchange corporation, price drops of these magnitudes translate into shareholder losses of between $50 million and $200 million.

But more damaging than the loss of money is the loss of trust and confidence by consumers in the Internet economy which so many of our nation's businesses depend upon. We can't risk losing the public's confidence in online e-commerce but consumers are beginning to rethink doing business on the Internet.

In the first six months of 2006, the home user sector was the most highly targeted sector, accounting for 86% of all targeted attacks. According to a survey of more than 10,000 households conducted by the Conference Board, 41 percent are purchasing less online because of security concerns. And according to a survey by the Cyber Security Industry Alliance, 32 percent of respondents strongly believe that their financial information may get stolen online.

We can't allow this trust to continue to erode. We can't continue to lose the public's confidence and expect to continue the robust digital lifestyle that we've come to enjoy. Trust ultimately, is the foundation of the online world.

But we have a long way to go in educating consumers. For example, a study by Small Business Technology Institute (SBTI) entitled, "Small Business Information Security Readiness," reveals a real lack of appreciation of the true economic impact of information security incidents and a lack of knowledge of cyber threats. Additionally, they find a lack of forward planning and matching investment required to maintain the security necessary to protect small businesses. Shockingly this study found that

over 74 percent of small businesses perform no information security planning whatsoever. Such a lack of knowledge and awareness is inhibiting the wide adoption of adequate information security protection.

Recommendations

Let me now discuss some actions that we believe Congress can improve our cyber security.

I. Awareness and Education

Educating our consumers, our small businesses, the operators of the critical infrastructure and all levels of government on the importance of protecting our systems is essential. We need a broad awareness campaign that reaches out to all users of the Internet.

The growing use of always-on broadband connections by home users and small businesses represents a significant amount of computing power, which left unprotected can be taken over and used as zombie machines to damage our networks and the hinder the commerce and services that flow through them.

At the least, these home users should deploy a minimum protection of firewall and anti-virus technology. The remote or wireless-connected worker is also becoming more prevalent and can unknowingly open up a corporate network to potential vulnerabilities and attack through unprotected connections.

Enterprises and government agencies should engage their employees in security awareness programs to ensure better protection of their systems. Whether it's reminding them not to post their passwords on a yellow sticky pad on their computer, or enacting corporate best practices to change those passwords on a regular basis making them difficult to break.

In an effort to better educate consumers, Symantec will participate in the October National Cyber Security Awareness Month initiative organized by the National Cyber Security Alliance (NCSA). As a founding sponsor of the NCSA, Symantec will also support the NCSA's national public service announcement campaign to promote online security among individuals, small businesses and schools.

The NCSA is a non-profit, public-private partnership consisting of businesses, consumer groups, government agencies and educational institutions dedicated to raising the awareness of cyber security issues and best practices. The NCSA provides tools and resources to empower home users, small business, and schools to stay safe online. More information about the organization and the October National Cyber Security Awareness Month can be found at www.staysafeonline.info.

At the enterprise and organizational level, the issue of IT security has for too long been an administrator or a CIO issue. This needs to change. Cyber security needs the attention of the CEO and the boardroom. Only then can we institute the necessary cultural change and focus enough attention and resources to truly address this issue. We urge the Committee to provide much needed resources to the agencies under its jurisdiction such as the Federal Trade Commission, the Department of Commerce and the Federal Communications Commission to promote cyber education to help better inform consumes of cyber threats.

II. Cyber Crime

We need to realize that protecting the Internet is really a global issue, one that requires better international cooperation. First, we need better resources for law enforcement to work on computer forensics, and we need cooperation from industry to assist prosecutors in building cases. Second, the ratification of the Council of Europe's cyber crime treaty is a good starting point but now that this framework is in place we need additional resources for international cybercrime enforcement, training funds and a single point of contact in the U.S. to coordinate such efforts. Third, industry should reach across borders when appropriate, to share information on best practices, threats and vulnerabilities, in order to gain a measure of early warning of potential attacks. Finally there should be a single point of contact in government so that those leaders can communicate at a peer level in times of major cyber attack.

III. Research and Development

Today, industry and government tends to look at the more immediate threats to our cyber infrastructure, rather than a holistic view of encompassing threats of today and tomorrow. It is a view that needs to change. As mentioned earlier, flash threats may be on us in the near future and we must be more proactive in our cyber security practices focusing on behavior blocking and better patch management, including the use of fast, safe and non-disruptive patching. Given the shrinking time from discovery to exploit, we should engage in projects like real-time vulnerability scanning, management and patching and we must do it together in partnership; industry government and academia alike. The Federal Government must focus on funding cybersecurity R&D to meet the constantly evolving threats that face our nation's critical infrastructure. And the Government must also lead by example, securing its own systems through the use of reasonable security practices.

IV. Clearly Defined Internet Response and Reconstitution Policy

The federal government needs a clearly defined Internet response and reconstitution policy for all agencies and departments. Public and private organizations that would oversee recovery of the Internet have unclear or overlapping responsibilities, resulting in too many institutions with too little interaction

and coordination. Also, existing organizations and institutions charged with Internet recovery should have sufficient resources and support. For example, little of the National Cyber Security Division (NCSD)'s funding is targeted for support of cyber recovery.

V. Secure Digital Control Systems for Physical Infrastructure

Our nation relies on a digitally controlled utility and commercial infrastructure such as the electrical transmission grid, oil and natural gas, water, waste water, chemicals, telecommunications, transportation, banking and finance – and many critical manufacturing processes. Remote control of distributed critical infrastructure occurs with Supervisory Control and Data Acquisition (SCADA) systems. These systems are designed to be open and interoperable; but their increasing use of the Internet for communications makes them vulnerable to cyber attack. Such attacks could have devastating consequences such as endangering public health and safety, according to the Government Accounting Office. We urge Congress to pass legislation to form a task force of key government agencies, appropriate regulators, experts in the cyber security field, and representatives from utilities and suppliers to meet and recommend concrete actions to improve the security of control systems supporting critical infrastructure.

VI. Direct a Federal Agency to Track Costs Associated with Cyber Attacks

No one in the field is satisfied with our present ability to measure the costs and probabilities of cyber attacks. There are no standard methodologies for the cost measurement, and study of the frequency of attacks is hindered by the reluctance of organizations to make public their experiences with security breaches. The lack of a methodology or measurement program also prohibits knowing how much national efforts to improve cyber security are working. We urge Congress to pass legislation directing the federal government to work with private industry on a methodology to measure the true cost of cyber attacks, and to track those associated costs as part of ongoing national economic assessment.

VII. Pass a National Data Breach Law and Consider Comprehensive Privacy Reform

The business community must join together with Congress to push for comprehensive privacy legislation. Some governments have already stepped to the plate. However, up until now, the U.S. government has been reactive – dealing with important parts of the issue on a piecemeal basis. Currently, U.S. privacy regulations focus on sensitive areas such as financial and health information and protecting children online. It's an approach that, ultimately, will result in a number of different confusing regulations. In light of the growth of identity theft and the rise of invasive threats like spyware, we need a comprehensive response that ensures that information is protected at every step along the way.

In this country, we need one, national data-breach law. Instead of the quilt of state laws, we need one federal law that protects all consumers from data breaches and requires businesses to put in place some

type of reasonable security measures. We urge Congress to pass a national data breach law this year that would require notification of affected consumers and would provide tough enforcement policies.

Conclusions

In closing, let me issue this challenge to industry, government and the individual users: We must take cyber security more seriously and we must do it together.

The increasing prevalence of blended threats and the potential for even more fast-spreading and damaging exploits is a serious threat to our nation's information infrastructure and the economic benefits that we derive from it. We need strong leadership from industry and government to promote awareness and education on cyber security, more resources for law enforcement to investigate and prosecute cyber criminals, strong research and development partnerships to tackle the challenges of future threats to the Internet, and more vigilance from business and governments by putting resources and support behind a proactive IT security program.

But most importantly we all as individual users of the Internet need to do our part, to protect cyber space. Experience shows that effective implementations of security solutions cost in the range of 6-8% of overall IT budgets. Few corporations outside of the finance sector, or government departments, have allocated such levels of funding to this critical need. It is time that we put our resources to work to minimize the risk of a serious disruption of our national cyber infrastructure.

Thank you and I look forward to your questions.